

Title (en)

Method and system for providing public key encryption security in insecure networks

Title (de)

Verfahren und System für öffentliche Schlüsselsicherheit in unsicheren Netzwerken

Title (fr)

Procédé et système pour la sécurisation avec chiffrement à clé publique de réseaux non-sûrs

Publication

EP 1748615 A1 20070131 (EN)

Application

EP 05300624 A 20050727

Priority

EP 05300624 A 20050727

Abstract (en)

A method for providing strong security in an insecure network (100), involving creating a payload associated with a data packet for transmission by a sending node (102, 108, 114, 120), determining whether the payload is associated with a unicast data packet, if the payload is associated with the unicast data packet encrypting the payload using a private key (106, 112, 118, 124) associated with the sending node (102, 108, 114, 120) to obtain a unicast encrypted payload, encrypting the unicast encrypted payload using a public key associated with a receiving node (102, 108, 114, 120) to obtain a double-encrypted payload, and transmitting the data packet including the double-encrypted payload to the receiving node (102, 108, 114, 120) over the insecure network (100)s.

IPC 8 full level

H04L 29/06 (2006.01)

CPC (source: EP US)

H04L 9/0822 (2013.01 - EP US); **H04L 9/0825** (2013.01 - EP US); **H04L 63/0428** (2013.01 - EP US); **H04L 63/0478** (2013.01 - EP US)

Citation (search report)

- [XY] US 5671285 A 19970923 - NEWMAN BRUCE D [US]
- [Y] US 5175765 A 19921229 - PERLMAN RADIA [US]
- [XY] STALLINGS W: "Cryptography and Network Security : Principles and Practice", 31 December 1998, PRENTICE HALL, NEW JERSEY, ISBN: 0-13-869017-0, XP002360130
- [Y] STALLINGS W: "Comunicaciones y Redes de Computadores", 31 December 1998, PENTICE HALL, SPAIN, ISBN: 84-89660-01-8, XP002360131

Cited by

CN104243161A; US7418596B1; US11381963B2; US2021385202A1; US11606342B2; US2023198970A1; US11929996B2; WO2020077502A1; US11265791B2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA HR MK YU

DOCDB simple family (publication)

EP 1748615 A1 20070131; US 2007028090 A1 20070201; US 7774594 B2 20100810

DOCDB simple family (application)

EP 05300624 A 20050727; US 33521706 A 20060119